Principles & Process of Risk/Opportunity Management

Applicable to an Architecture Environment

Introduction

Along with Risk, always read "Opportunity"

- **Risk Management (RM)** is an organized, systematic decision-making process that efficiently identifies risks to the achievement of Program goals, assesses those risks, and leads to their reduction or elimination
  - **Vital** to effective Program communications and leadership
- *Opportunity management* (OM) is a parallel concept
  - "Flip side" of RM – good things happen if it works (vice bad things not happening)
  - OM is subject to the same principles & techniques as RM

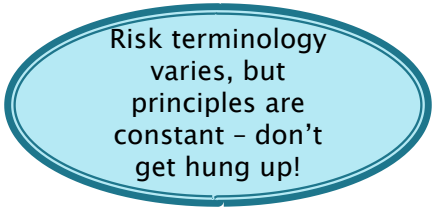
RM Enables Sound *Planning*

- Like planning, good RM maximizes the likelihood that a program will meet all its requirements

- How many times have you heard these non-plans:
  a. "We'll cross that bridge when we come to it."
  b. "We'll make a prudent decision at the appropriate time."
  c. "We're waiting for guidance from HQ about that."

If you think managing risks is a hassle, try NOT managing them!

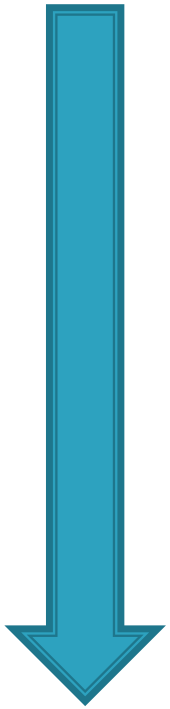
A Key Distinction



- **Risk**: A circumstance which has both the potential to occur, and a negative consequence for Program or Project success should it do so
  - Types of risks: Cost, Schedule, Technical (Performance), Program (Reputation of program)
  - Risk tends to vary directly with uncertainty
- **Issue (AKA *Problem*)**: A Risk that has already occurred, or whose probability of occurring in the near term is 100 percent.
  - RM addresses both Risks and Issues

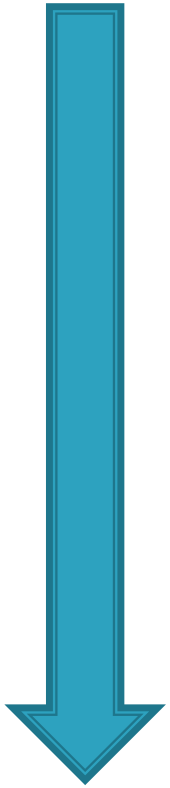
Spectrum of RM Models (I)

Passive RM
Ill-resourced
Informal
Collective
Unaccountable



- **"Risk POC" Model:** Enterprise-level POC collates and compares the risks brought forward by Projects; risk analysis typically episodic, under-resourced
  - Cheapest and quickest model to implement
  - Risk POC is mid-grade and maybe part-time -- no charter, RM tool, or Deputy RM
  - RM forums (meetings) are hard to arrange, and scope unclear; little new content
- **"Parallel Management" Model:** Projects conduct own RM process, largely disconnected from that at enterprise level.
  - Enterprise Risk Cell is bigger, but must work hard to stay informed
  - Often bypassed by Projects with something to hide
  - Lack of full coordination of risk reports can lead to resentment between levels

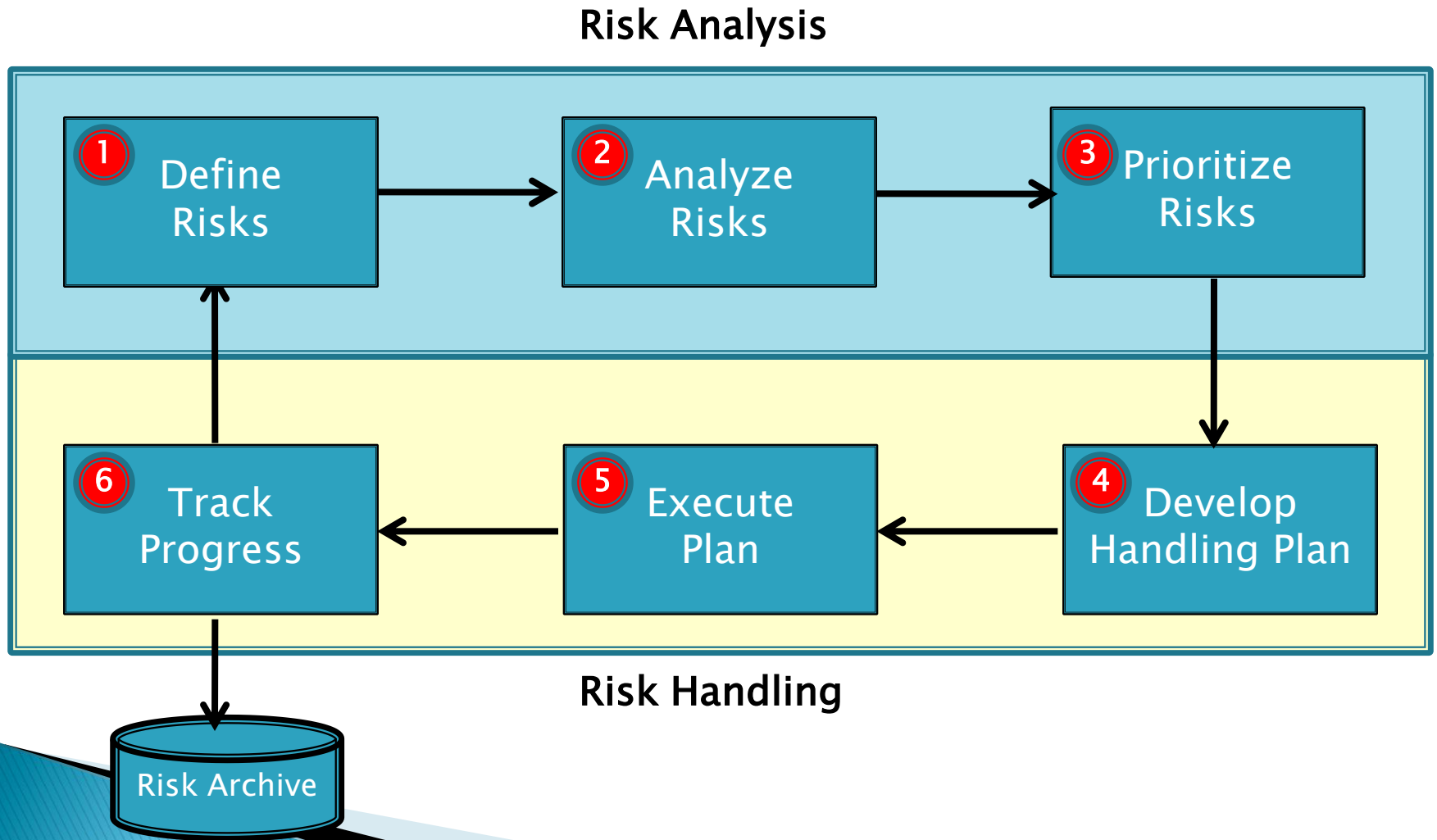
Spectrum of RM Models (II)



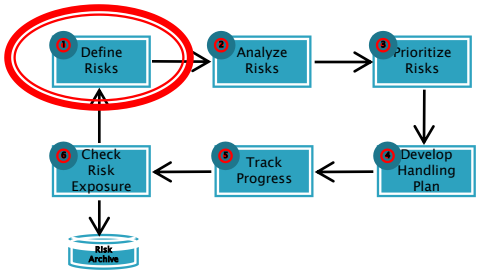
Active RM
Responsible
Resourced
Formal
Accountable

- **"Two-Stage RM" Model**: Project risk POCs document & analyze Project risks, then turn over to enterprise RM to add enterprise flavor and conduct summary reporting.
  - Projects lose control of risks upon turnover – can be blind-sided if insufficient prior coordination by RM
  - Takes longer than the above two methods to consolidate inputs, prep/coord. Reports
- **"RM Empire" Model**: Risk Manager attempts to document, analyze, report all key risks at every level
  - Impractical & dangerous – sets up enterprise RM as single point of failure

RM Cycle Overview

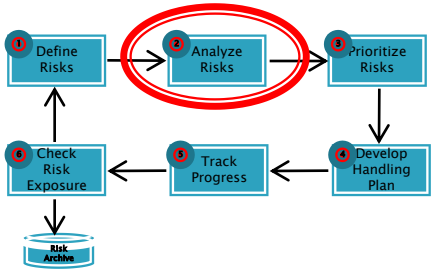


Step 1: Define Risks

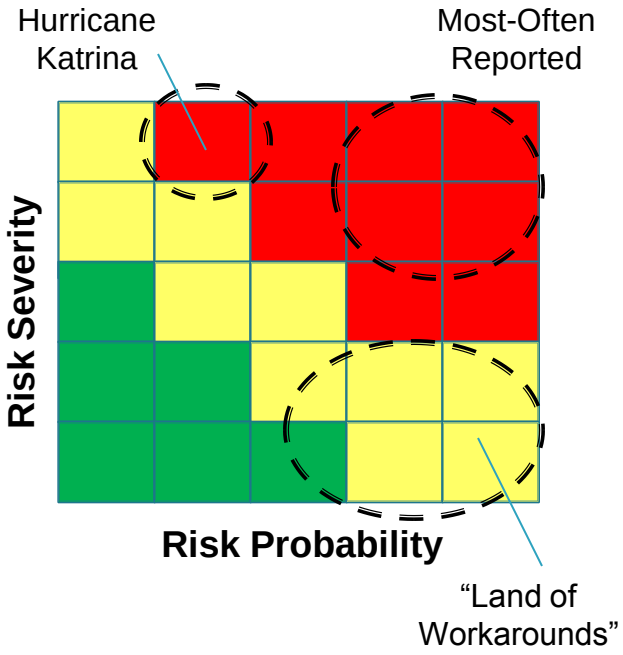


- Enumerate known risks
- Search for risks not immediately obvious
- Identify dependencies among risks
- Write actionable risk statements, of the general form:
  - "**IF** [immediate cause], **THEN** [risk condition to occur], **RESULTING IN** [consequence] **TO** [entity] **WITHIN** [timeframe] and **LASTING** [duration]."
  - Example: "If Vendor X does not deliver the Sepsis Assembly on time, then preparations for Segment FAT will be delayed, resulting in delay of FAT by the Development Team for approximately three weeks."
- Designate an "Owner" for each risk

Step 2: Analyze Risks

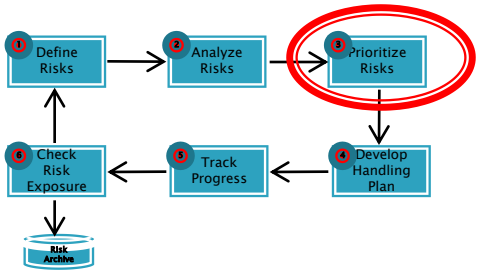


- Where possible, *quantify* risks to permit direct comparison, reduce subjectivity
  - Give scary numbers and ranges plain-English labels (e.g., "High","Very Probable") to aid understanding & acceptance
- Consider using a 5x5 Risk Matrix (example at right), or similar to summarize risk exposure
  - Extended Red range draws attention to more Severe risks, no matter how Probable
  - Most other risks are either worked-around or dismissed
  - Danger lies in marginal cases – "Hurricane Katrina"
  - Avail. resources and relative risk-aversion of Program leaders determine what (if anything) is done
- Search for & address root causes
  - One "high-leverage" mitigation action can prune away many risks which have same root cause



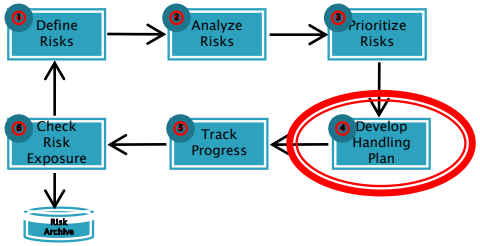
Regions of a 5x5 Risk Matrix

Step 3: Prioritize Risks



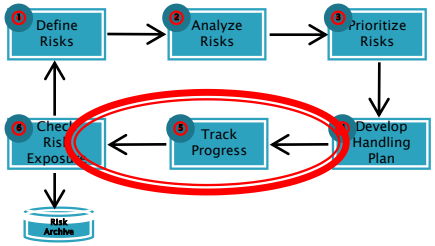
- Purpose is to focus & apply limited resources (both financial and personnel) to handle greatest threats
- Nominated by risk originator, reviewed by a group
- Highest Probability x Consequence are *usually* addressed first
  - "Final" priority isn't result of raw calculation, but common sense!
  - Compare risks in their proper context
  - High risk to a Project may not be same to the Enterprise

Step 4: Handling Plans



- Five Strategies:
  - **Avoid** – change conditions under which the risk arose
  - **Transfer** – get another organization to agree to accept the risk as its own
  - **Control (Mitigate)** – work to reduce Prob. X Consequence of risk by positive action
  - **Watch (Monitor)** – Allow actual Prob., Consequence of risk to become more clear
  - **Assume (Dismiss)** – Re-define the risk as simply part of the "cost of doing business"
- Handling Plan is based on one or more of these Strategies. It must be actionable:
  - What Action Steps, taken when, by whom…
  - Include a Risk Point-of-Contact (POC) and Periodicity for re-examination
  - Times are usually stated in terms of engineering/acq. milestones: PDR, FAT, etc.
  - *Contingency Plans* are paired with each of the most serious ("red") risks
    - Attempt to implement our Handling Strategy failed – now what?
- Choice of Handling Plans constrained by risk Priority, business rules
  - EX: "We never *Assume* any "red" risks, OR those potentially affecting personnel safety"
  - EX: "We don't bother to *Avoid* or *Control* "deep green (1/1) risks."

Step 5: Execute Risk Plan

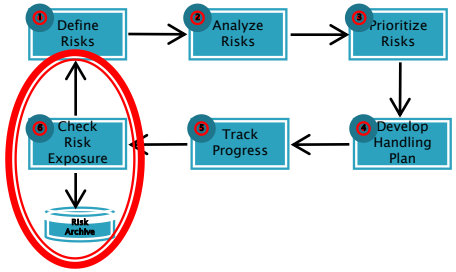


- Adopt standardized reporting format (largely tool-dependent)
- Designate recurring venues for risk reporting
- Maintain political support for RM – don't be seen as "tattletale" on risky/under-performing Projects

1. Project Leads feed Risk Manager their "Top 10" risks in advance
2. Risk Manager summarizes risk situation, reports key enterprise risks
   - Briefing, RM Portal, personal communications with management
   - Concentrate on dependencies between/implications for enterprise Developer-level risks, and risks with time-to-onset of $\leq$ 90 days
   - Risk Manager provides Risk Tip-offs directly to PM as required (even out-of-cycle with normal risk reporting)
3. Clients (GPOCs) are kept in-loop with respect to controversial risk I.D.s, analyses, Handling Plans

One possible implementation

Step 6: Track Progress



- Review Handling Plans routinely with management
- As Action Steps are completed, revisit the analysis
- Need to re-evaluate in any case if:
  - Key milestone is approaching
  - New stakeholder appears
  - Program/Project enters new phase
- *Close* risks, with explanation, to an RM Archive
  - Don't be afraid to mothball risks, but do so for good reason
    - If RM process is truly effective, this will happen frequently
    - Program must attend closely to the number, uniqueness, complexity, and fidelity (detail) of risks under management…
    - …and even MORE closely to the risks that get *reported*

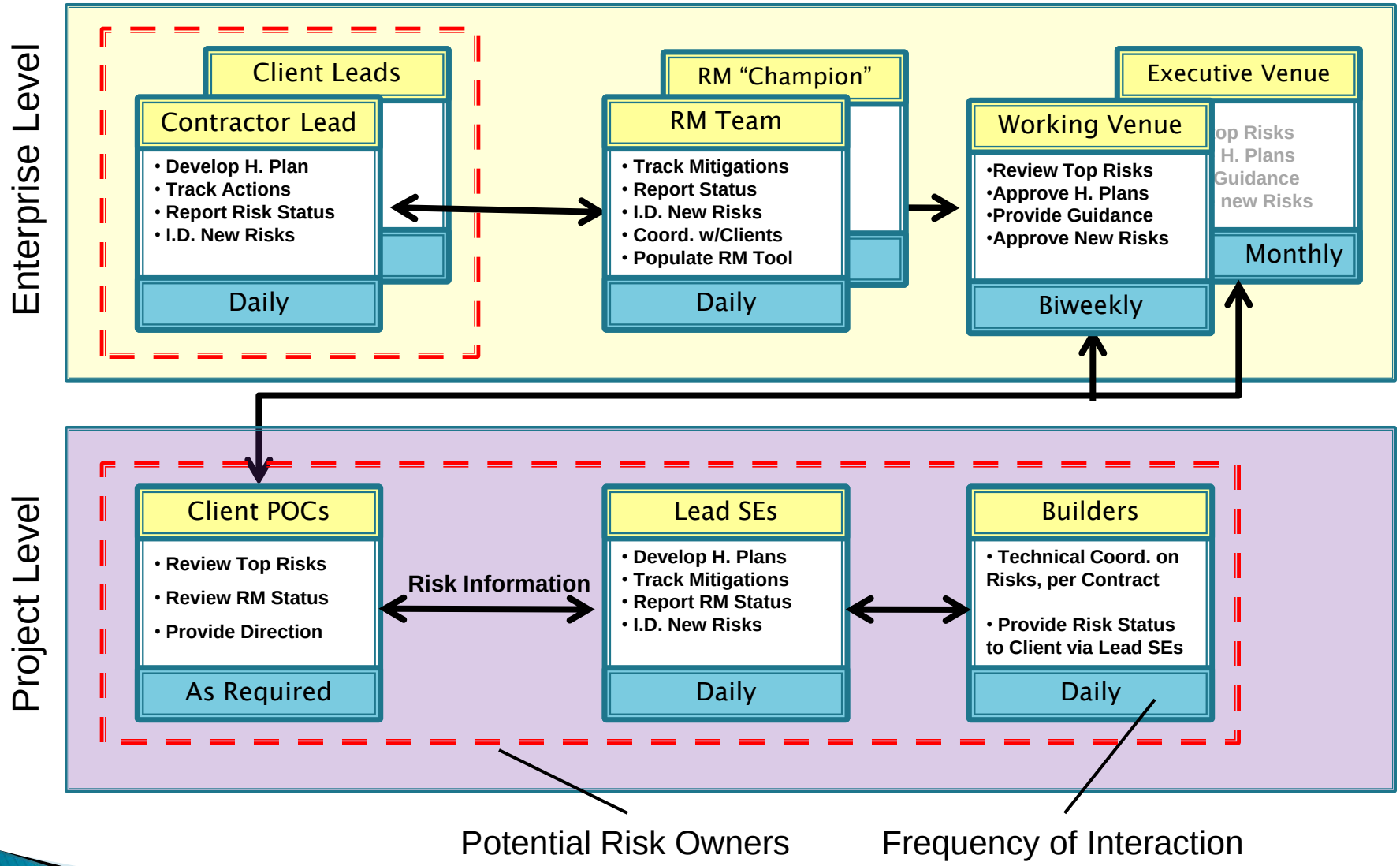
Organizational Deficiencies Typically Noted with Respect to RM

- Inconsistent risk tracking (process Steps 5, 6)
  - Risks fall through the cracks
- RM resource imbalance
  - RM structure at enterprise level is much more/less robust WRT that at Project/Segment level
- RM has no **center of gravity**/foothold
  - Responsibilities are too dispersed
  - No designated Risk Manager (or, "all" are claimed to be RMs!)
  - Nonexistent/non-integrated risk communications strategy
  - No RM "champion" among key Clients/stakeholders
- No **RM culture**
  - Many unnecessary risks are routinely tolerated
- Insufficient fidelity to risk analyses
- Opportunity Management is haphazard
- RM training not addressed

Professionals don't brush off risks!

Try to reduce risk a little *with every decision*

Typical RM Activities & Interactions



RM Team or collective bodies (e.g., boards) should not "own" risks

Key RM Roles (I):
Enterprise Risk Manager (RM Team Lead)

- Prepares, implements, updates *RM Plan*
- Chairs RM meetings, speaks for RM at other mtgs. as required
- I.D.s and documents *enterprise* risks/opportunities
- Summarizes risk inputs from lower levels
- Leads task of making inputs to RM tool
- Advises & assists Project level in complying with risk process
- Supervises & helps rate Deputy Risk Manager
- Creates & delivers initial Risk Process training to organization, and to new personnel as required thereafter

Responsibilities

- Extensive systems engineering (SE) and integration background
- Lots of Domain (substantive and/or process) experience
- RM experience preferred
- Excellent writer/briefer;
- "Street cred" and respect within organization
- Able to co-locate with PMO and/or greatest source of risks
- Able to devote full time to RM

Typical Qualifications

Key RM Roles (II):
Deputy Enterprise Risk Manager

- Assists Enterprise Risk Manager as required
- Maintains RM infrastructure (app., server, RM Portal, etc.)
- Trains selected personnel in use of RM tool
- Makes substantive inputs to RM tool (secondary duty)

Key RM Roles (III): Contractor Lead (PM/DPM)

- Review & approve risk reports in advance
- Act promptly on Risk Tip-offs
- Guide RM personnel re: priorities for analysis
- Conduct general oversight of how Handling Plans are implemented
- Evaluate (rate) the other RM players on contractor team

Key RM Roles (IV): Contractor Lead SEs, Integrators

- Define & analyze Project-level risks
- Propose Handling Strategies
- Coordinate on section(s) of Risk Manager's risk status reports/forecasts that deal with their own Projects
- Work with Risk Manager and Deputy to improve RM process at the Project level
- Provide Risk Manager with timely Risk Tip-offs
- In the case of a system development program, gather data on both new and existing risks from Builders (system fabricators) and provides it to RM
- Lead implementation of Handling Strategies for risks they "own"
- Report status with the frequency & level of detail agreed with RM

Key RM Roles (V):
RM "Champion"

Typically a senior Client

- Aggressively promotes RM effort throughout the organization
- Tracks & reports savings in time, money, operational risk due to RM
- Helps ensure RM gets the resources & attention it needs to be effective
- Critiques, re-directs RM effort as needed

Implementing RM: 12 Guiding Principles

1. Establish an enterprise perspective on risks, opportunities
2. Promote development of a risk-managing culture
3. Don't "break" whatever RM mechanisms are already working well
4. Rely on persons closest to the data, *for data* at all levels
5. Leverage technology/tools where appropriate
6. Fix the most troubled "steps" (RM activities) first
7. Establish momentum: roll out at least an interim RM capability *ASAP*
8. Don't let the RM process impede system development
9. Demonstrate RM's value-added early
10. Maintain political support for RM
    1. Don't let Risk Manager be perceived as "tattletale" on risky/under-performing projects
11. Keep stakeholders informed of RM progress
12. Minimize footprint of the RM effort, consistent with its effective implementation

Dedicated RM Tool

- Software package (commercial, proprietary, or home-grown)
- Makes the RM effort *scalable*
  - Many dozens of risks usually need to get documented, tracked, reported – hard to do with MSOffice
- Used to configuration-mange (CM) risk descriptions, handling plans, etc.
  - Consistent characterization of risks
- Instant graphical outputs promote comprehension, comparison of risks
- Allow stakeholders to review risk status at will online (if network-enabled)
- Allows decentralized input of risk data (if network-enabled)
- Variable permissions can lock some in, others out, preserve integrity of data
- Typically extracts metrics (measures) upon which to judge effectiveness of the RM process
- Modern commercial tools are quite sophisticated

Without a serious risk tool, it's not serious risk management

Assumptions
(Factors Leading to Successful RM)

1. All key players participate
   - Risk Champion, Client leads, Lead SEs, Project managers
   - Lack of cooperation brings:
     - Low completeness & currency of risk write-ups
     - Marginalized risk program that falls out-of-step with reality
     - ***Bad decision-making***
2. RM cell is adequately resourced (staff, tool, space, comms)
3. Risk Manager is dynamic, personable, discreet
4. Relevant Program Management and Communications plans are themselves implemented to acceptable degree
5. RM Execution Plan is respected & followed
6. Organization feels the need to change

Final Thought
for Prospective Risk Managers

•"Attempting to achieve complex goals in fast-moving, unpredictable environments is humbling…Managers expect to be able to identify, plan for, and influence all the variables and players in advance, but they can't. Nobody is that smart or has that clear a crystal ball. They can, however, create an ongoing process of learning and discovery, challenging the people closest to the action to produce results – and unleashing the organization's collective knowledge…."

Matta & Ashkenas (HBR, Sept. 03)